AMENDMENTS TO THE CLAIMS

1. (Currently amended) ~~In a computer system~~ A method for providing access to at least one secure resource upon authentication of a user where said user authentication is performed by an authentication server in remote communication with a client in use by said user, ~~a~~ the method ~~of saving said user authentication for use when said authentication server is unavailable, the method~~ comprising the steps of:

(a) submitting a user authentication request to said authentication server;

(b) in response to a successful user authentication~~;~~:

(b1) receiving an authenticated user credential which ~~Is~~ is unique to said user

(b2) storing said authenticated credential on said client utilizing a security method to prevent tampering with the credential; and

(b3) using said authenticated credential to access said at least one secure resource;

(c) in response to an unsuccessful user authentication:

(c1) determining whether said authentication server is in operative communication with said client;

(c2) in response to a step (c1) determination that said authentication server is not in operative communication with said client:

(c2a) searching said client for a stored authenticated credential corresponding to said user;

(c2b) in response to a step (c2a) finding of an authenticated credential corresponding to said user, using said stored authenticated credential to access said at least one secure resource without further authenticating the credential with the server or other authenticating entity while said authentication server is not in operative communication with said client; and

(c2c) in response to not finding in step (c2a) an authenticated credential corresponding to said user, failing the user authentication request.

2. (Currently amended) The method of claim 1 further comprising the steps of:

(c3) in response to a step (c1) determination that said authentication server is in operative communication with said client:

(c3a) erasing from said client any stored authenticated credential corresponding to said user; and

(c3b) failing said user authentication request.

3. (Cancelled)

4. (Currently amended) The method of claim 1 wherein said security method is encryption of the credential, further comprising the steps of:

decrypting the credential;

determining whether the decrypted credential has been tampered with; and

failing the user authentication request in response to a determination that the decrypted credential has been tampered with.

5. (Currently amended) The method of claim 1 wherein said security method is Public Key Infrastructure, further comprising the steps of:

decrypting the credential with a key stored on the client;

determining whether the decrypted credential has been tampered with; and

failing the user authentication request in response to a determination that the decrypted credential has been tampered with.

6. (Currently amended) The method of claim ~~1~~ 5 wherein said Public Key Infrastructure ~~security method~~ is hardware-based ~~Public Key Infrastructure~~.

Claims 7-9. (Cancelled)

10. (Currently amended) ~~In a computer system~~ A method for providing access to at least one secure resource upon authentication of a user where said user authentication is performed by an authentication server in remote communication via a secure gateway with a client in use by said user~~, a method of caching said user authentication for use when said authentication server is unavailable~~, the method comprising the steps of:

(a) submitting a user authentication request to said authentication server;

(b) in response to a successful user authentication;

(b1) receiving an authenticated user credential which is unique to said user;

(b2) storing said authenticated credential on said client utilizing a security method to prevent tampering with the credential;

(b3) storing said authenticated credential on said gateway utilizing a security method to prevent tampering with the credential; and

(b4) using said authenticated credential to access said at least one secure resource;

(c) in response to an unsuccessful user authentication:

(c1) determining whether said authentication server is in operative communication with said client;

(c2) in response to a step (c1) determination that said authentication server is not in operative communication with said client; determining whether said gateway is in operative communication with said client;

(c3) in response to a step (c2) determination that said gateway is not in operative communication with said client:

(c3a) searching the client for an authenticated credential corresponding to said user;

(c3b) in response to finding an authenticated credential corresponding to said user in step (c3a), using said authenticated credential to access said at least one secure resource without further authenticating the credential with the server or the gateway or another authenticating entity while said gateway is not in operative communication with said client; and

(c3c) in response to not finding an authenticated credential corresponding to said user in step (c3a), failing the user authentication request.

11. (Currently amended) The method of claim 10 further comprising the steps of:

(c4) in response to a step (c2) determination that said gateway is in operative communication with said client:

(c4a) searching the gateway for an authenticated credential corresponding to said user;

(c4b) in response to finding an authenticated credential corresponding to said user on the gateway in step (c4a), using said authenticated credential to access said at least one secure resource without further authenticating the credential with the server or gateway or other authenticating entity;

(c4c) in response to not finding an authenticated credential corresponding to said user on the gateway in step (c4a), failing the user authentication request;

(c5) in response to a step (c1) determination that said authentication server is in operative communication with said client:

(c5a) erasing from the client any authenticated credential corresponding to said user;

(c5b) erasing from the gateway any authenticated credential corresponding to said user; and

(c5c) failing the user authentication request.

Claims 12-15. (Cancelled)

16. (Currently amended) The method of claim 11 wherein at least one of said step (b2) and step (b3) security ~~method~~ methods is encryption of the credential, further comprising the steps of:

decrypting the credential;

determining whether the decrypted credential has been tampered with; and

failing the user authentication request in response to a determination that the decrypted credential has been tampered with.

17. (Currently amended) The method of claim 11 wherein at least one of said step (b2) and step (b3) security ~~method~~ methods is Public Key Infrastructure, further comprising the steps of:

decrypting the credential with a key stored on the client;

determining whether the decrypted credential has been tampered with; and

failing the user authentication request in response to a determination that the decrypted credential has been tampered with.

18. (Currently amended) The method of claim ~~11~~ 17 wherein said Public Key Infrastructure ~~security method~~ is hardware-based ~~Public Key Infrastructure~~.

19. (New) The method of claim 10 wherein the authenticated user credential is a light-weight directory access protocol.

20. (New) The method of claim 10 wherein the wherein at least one of the steps (c3b) and (c4b) of using said authenticated credential to access said at least one secure resource further comprise the steps of:

determining an elapsed time since a previous remote server authorization;

comparing the elapsed time to a threshold time; and

in response to the elapsed time exceeding the threshold time, failing the user authentication request.

21. (New) The method claim 10 further comprising the steps of:

assigning a high sensitivity level or a low sensitivity level to the at least one secure resource; and

failing the user authentication request if the at least one secure resource sensitivity level is the high sensitivity level unless the authenticated credential is found on either the server or the gateway.

22. (New) The method of claim 1 wherein the authenticated user credential is a light-weight directory access protocol.

23. (New) The method of claim 1 wherein the step (c2b) of using said authenticated credential to access said at least one secure resource further comprise the steps of:

determining an elapsed time since a previous remote server authorization;

comparing the elapsed time to a threshold time; and

in response to the elapsed time exceeding the threshold time, failing the user authentication request.

24. (New) The method claim 1 further comprising the steps of:

assigning a high sensitivity level or a low sensitivity level to the at least one secure resource; and

failing the user authentication request if the at least one secure resource sensitivity level is the high sensitivity level unless the authenticated credential is found on either the server or the gateway.

25. (New) A computer system, comprising:

an authentication server;

a client in remote communication with the authentication server; and

at least one secure resource in communication with the client;

wherein the client is configured to store on the client a first authenticated credential received from the authentication server in response to a successful user authentication by utilizing a security method to prevent tampering with the credential; and

wherein the client is configured to use the stored first authenticated credential to access the at least one secure resource without further authenticating the first credential with the server or other authenticating entity while the authentication server is not in operative communication with the client.

26. (New) The computer system of claim 25, further comprising a secure gateway machine connected between the authentication server and the client;

wherein the gateway machine is configured to store a second authenticated credential on the gateway received from the authentication server in response to a successful user authentication by utilizing a security method to prevent tampering with the second credential; and

wherein the client is further configured to use the second authenticated credential to access the at least one secure resource without further authenticating the second credential with the server or other authenticating entity while the authentication server is not in operative communication with the gateway.

27. (New) The method of claim 26, wherein at least one of the client security method and the gateway security method is encryption, and wherein the client is further configured to decrypt the first credential or the second credential, determine whether the decrypted credential has been tampered with. and fail a user authentication request if decrypted credential has been tampered with.

28. (New) The method of claim 26, wherein at least one of the client security method and the gateway security method is Public Key Infrastructure, and wherein the client is further configured to decrypt the first credential or the second credential with a key stored on the client, determine whether the decrypted credential has been tampered with, and fail a user authentication request if decrypted credential has been tampered with.